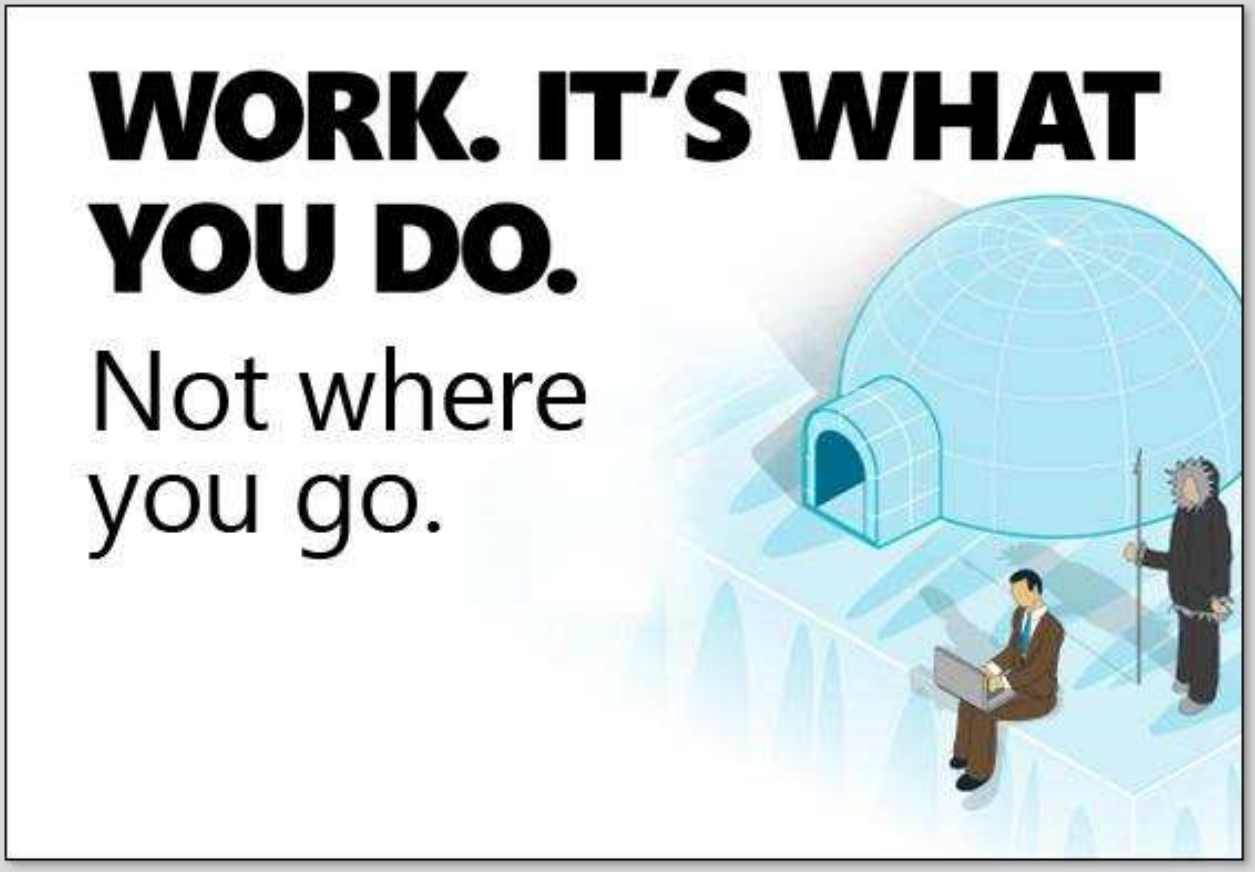
Microsoft



TELEWORK PLANNING CONSIDERATIONS:

A RISK-BASED APPROACH FOR IT MANAGERS

A Microsoft U.S. government white paper
June 2011

This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

CONTENTS

LIST OF TABLES

DEVELOPING A RISK-BASED APPROACH TO TELEWORK

With the passage of the Telework Enhancement Act of 2010 (H.R. 1722), your agency must be prepared to support a more mobile workforce—while protecting your critical network infrastructure and assets. In a rapidly changing threat landscape, you must develop risk-based strategies for providing secure and reliable access and services to teleworkers.

Government mandates have been pushing agencies to review their risk management profile and to adjust to the changing work environment. To support the new telework mandate, you must have a plan for risk mitigation even while you deliver new services to a growing mobile workforce. The task may seem overwhelming until you realize that risk management is not just a technology issue but also a people and process issue.

If your agency is like many, you probably already provide some of the technology you need for telework. For example, an existing Microsoft Exchange Server deployment can support remote messaging services, a foundation for telework. And you probably already deploy firewalls, multifactor authentication, remote access services, and other defense and protection strategies.

To manage risk in a telework environment, you can start by defining your business objectives and telework service deliverables, just as you would for any project. In a remote access scenario, these are your endpoints—the devices and services you provide. With an understanding of the choices you have at the endpoints, you can assess the risk to your assets by performing *threat modeling*, a methodical review of your systems to discover and correct security problems at the level of design, configuration, and deployment. Then you can build in appropriate security measures to mitigate discovered risks.

What's new for IT

Even though congress has advocated for telework policies for more than a decade, a review in 2007 by the Government Accountability Office (GAO) showed that, of the four agencies they reviewed, none were managing their telework programs based on measurable results. With this act, however, agencies must assess the impact of telework—something that IT staff can directly affect.

For example, if you provide a solid remote access solution, you support your agency's continuity of operations (COOP) planning. By providing familiar software and tools that workers have access to anytime and anywhere, you help support their productivity.

IT groups can also help foster positive attitudes toward telework by demonstrating useful technologies, such as presence and unified communications, to managers and employees.

ASSESSING RISK IN TELEWORK

To keep systems safe, you use computer firewalls, run antivirus monitoring, encrypt documents and email messages, and deploy other technologies, too. However, telework security is not just a technology issue nor is it something to add to IT systems after the fact. You need a flexible, multifaceted approach to managing risk.

Before your agency starts planning telework solutions, you must:

- Define the assurances and security objectives you want to provide to your enterprise and its users.
- Develop a risk profile for the IT assets (endpoints, services, applications, and data) you must protect in a telework scenario.
- Determine your risk tolerance or appetite—that is, the risks that are acceptable and unacceptable.

There are many ways you can support teleworkers, but first you should develop a risk model. Then you'll have a framework for discussions about policy, security controls, and the services you want to provide to teleworkers—and, finally, the technologies that will enable these.

In any system, the greatest risks tend to stem from areas least under your control. With telework, those areas are often the endpoints of your network—the devices that workers use to access government resources—and the connections to your network. Your endpoints may be desktop PCs, laptops, smartphones, or other mobile devices. Employees may use government-furnished equipment (GFE) running known configurations, or they may use their own devices. They may connect from home Internet connections or from public WiFi hotspots. You need a way of assessing the risk to your network from all these types of devices and connection scenarios.

You may not be able to eliminate the threats associated with remote access across a public infrastructure—new types of Internet attacks seem to arise with growing frequency. However, you can devise strategies to manage your risks at the endpoints and connections and then design and deploy telework services accordingly.

Telework abbreviations

GFE: *Government-furnished equipment*. Provide devices with a known configuration to help mitigate risk.

PII: *Personally identifiable information*. Use encryption to help protect data in motion and at rest—on hard drives and in databases.

SDP: *Sensitive data protection*. Verify authorization and limit access to sensitive data.

SLA: *Service level agreement*. Set teleworkers' expectations through guidance and training.

STRIDE: ***S**poofing, **t**ampering, **r**epudiation, **i**nformation disclosure, **d**enial of service, **e**levation of privilege*—risks your threat model must consider.

VPN: *Virtual private network*. Use to send data across secured and encrypted private channels between two points via the Internet. Newer technologies, such as Windows 7 Direct Access, provide similar functionality without the need for a separate VPN.

STEP 1: START AT THE ENDPOINTS

Whether your telework risk tolerance is low, high, or somewhere in between, you need a set of objective parameters to craft useful risk profiles to which you can apply risk mitigations. A simple method leverages Microsoft Active Directory as a basis for endpoint profiling. This approach gives you two profiles:

- **Managed devices.** This profile includes devices that are members of an Active Directory forest (for example, GFE smartphones or agency-issued laptops). During the logon process, a managed device can state its compliance with agency policies. If not in compliance, it can be brought into compliance, giving this type of device a lower relative risk profile.
- **Unmanaged devices.** This profile includes devices that are not members of an Active Directory forest, such as a worker's home PC or a personally owned mobile device. Because you do not know whether they comply with your security policies, these devices potentially represent a higher risk.

For example, consider an agency-issued laptop running a known configuration that is a member of the organization's Active Directory forest. Through Active Directory, the laptop receives policies, configuration rules, and software updates. With this infrastructure, you can have a high degree of assurance that the laptop is well managed, and you can validate its compliance with agency policies.

This simple classification—managed versus unmanaged—gives you a straightforward framework in which you can develop a more granular risk profile. By subdividing the classifications as necessary, you can fit them to your organizational processes, policy selections, and policy enforcement solutions.

Microsoft security platforms

When making services available to teleworkers, you must protect your network. Microsoft provides these backbone solutions for telework scenarios:

- Network Access Protection (NAP) components in Windows Server 2008, Windows 7, and Windows Vista provide a platform to help ensure that client computers on a private network meet your requirements for system health.
- DirectAccess, introduced in the Windows 7 and Windows Server 2008 R2 operating systems, allows remote users to access enterprise shares, websites, and applications without connecting to a virtual private network (VPN).
- Forefront Unified Access Gateway 2010 is an endpoint security solution that delivers anywhere access to software services, performs granular endpoint health detection, and is integrated with NAP policies.
- Forefront Threat Management Gateway is a web gateway that offers multiple layers of continuously updated protections, including URL filtering, anti-malware inspection, intrusion protection, application proxy, and HTTP/HTTPS inspection.

STEP 2: ESTABLISH SERVICE LEVELS

Based on a device's risk profile, you can determine the *scope of access* it may receive to agency services. Scope of access refers to the type and number of services a teleworker requires and will vary by job role and other considerations, such as available bandwidth. This scope defines the service level agreement your organization can provide to teleworkers.

In general, you must consider two levels of service:

- **Full** access to agency network and services.
- **Limited** access to a subset of services or access for a limited duration.

With a limited SLA, you have many options for lightweight solutions that give teleworkers sufficient access with a lower risk profile. For example, you can provide access to one or two key productivity applications, such as collaboration solutions, email, or line-of-business applications.

STEP 3: SET UP A RISK-BASED SERVICE STRATEGY

Together, risk profiles and service levels form a matrix of telework options. Now you have a clear framework in which to discuss risk and to define subsequent policies. With those in place, you can begin to investigate technological solutions that help you fill any gaps in the way that telework services access your network infrastructure, other services, and assets.

The goal in developing a risk-based approach to telework is to leverage existing technologies and new investments in a cost-effective manner across both managed and unmanaged devices and to then use a layered approach to protection. You can use the tables that follow to explore various scenarios for managed and unmanaged telework devices that require full or limited access.

Enterprise Security Management Life Cycle

Microsoft recommends a life cycle approach to security, which combines the strategy of constant process improvement with the operational tactics of continual monitoring and defense in depth. There are four steps in the cycle:

- **Protect** information assets everywhere while providing access to those who need resources from anywhere. By understanding your priority assets, along with their risks and vulnerabilities, you can devise policies to manage risks and then implement appropriate solutions based on your policies.
- **Detect** intruders and monitor continuously for unauthorized access. Start by setting a baseline for normal activity. Then you can use tools, technologies, and best practices to manage and monitor your protection solutions and detect malicious events.
- **Respond** immediately to a detected threat, assess the extent of damage, and determine whether exfiltration of enterprise data occurred.
- **Recover** any lost data or configuration information, analyze the event, and learn how to prevent similar incidents from recurring. Not only should your IT organization have a plan for recovering a secure state, but also it must reestablish trust in your IT assets.

Table 1. Strategies for providing full network access

Device	Risk profile and suggested solutions
Managed GFE device	A PC running an approved configuration, such as the U.S. Government Configuration Baseline (USGCB), that includes up-to-date software, such as Windows 7, would have a relatively low risk profile. It could be approved for teleworkers who need full network access. With this configuration: ▪ Take advantage of Windows 7 Direct Access technology, a cost-effective way to establish a VPN when a device has a connection to the Internet. DirectAccess is a cornerstone of the Microsoft strategy for remote access services. ▪ Provide multifactor authentication on the server side to verify device compliance and user authentication. For example, deploy Windows Server 2008 R2 with NAP. ▪ Use a smart card on the client side that complies with Federal Information Processing Standards (FIPS) Publication 201.
Managed legacy device	Devices running older versions of software, such as Windows Vista or Windows XP SP3, may present a higher risk profile, even if well managed. To support teleworkers who require full network access, you need to use a VPN solution capable of verifying device compliance and authenticating identities. With this configuration: ▪ Deploy additional edge protection against Internet-based threats. You can use a gateway solution, such as Forefront Threat Management Gateway. ▪ Look for an endpoint detection solution that helps you verify compliance with your security policies while offering network management benefits, such as Forefront Unified Access Gateway.

Table 2. Strategies for providing limited network access

Device	Risk profile and suggested solutions
Managed legacy device	The risk associated with devices running older versions of operating systems is mitigated to some degree by limiting access. With this scenario: ▪ Make devices connect via secure socket layers (SSL) VPN with support for smart card user authentication. ▪ Create an access portal to host selected services. For example, you can use Forefront Unified Access Gateway to host a collection of services, which you can publish using remote desktop services. ▪ Use this type of lighter weight solution for unmanaged devices, as well, by adding a solution for endpoint detection and cleanup.
Managed mobile device (smartphone)	If GFE, a well-managed smartphone is limited primarily by its screen and keyboard size. It may be capable of running a wide variety of business apps, but they must be designed for small screen rendering and non-mouse navigation. With this scenario: ▪ Ensure that devices receive and implement your policies from Active Directory. ▪ Enable access to messaging and collaboration solutions and selected line-of-business applications that have a mobile interface.

Table 3. Strategies for providing access from unmanaged devices

Device	Risk profile and suggested solutions
Employee-owned home PC	Unmanaged devices may pose a higher risk to your network than those with known configurations. The goal is to mitigate the risk as much as possible by limiting services while requiring and enforcing necessary policies. In this scenario: ▪ Create an access portal to host selected services. For example, you can use Forefront Unified Access Gateway to host a collection of services, which you can publish using remote desktop services. ▪ Enforce applicable policies. For example, ensure that PCs have all the current software updates and that up-to-date antivirus protection is installed and running before you allow user authentication. ▪ Consider requiring the use of a smart card and install the needed middleware. For example, OWA supports the use of personal identity verification (PIV) cards for user authentication.
Non-employee owned PC	A very high-risk profile, this type of unmanaged device should be considered in your COOP and risk analysis, even if you do not support it for telework. In this scenario: ▪ Provide limited access only if you can verify and enforce software updates and antivirus use. ▪ Enforce security compliance using Group Policy Objects (GPO) on the unmanaged device.

Microsoft Outlook solutions you may already have

Organizations that use Outlook for email services may have a telework-ready solution close at hand. You can deploy a simple, lightweight messaging solution using Outlook in two ways:

- Configure Outlook 2010 to use Outlook Anywhere, which enables user accounts to connect to Microsoft Exchange Server 2003 or a later version over the Internet without using VPN connections. In earlier versions of Outlook, this capability is known as remote procedure call (RPC) over Hypertext Transfer Protocol Secure (HTTPS).
- Use Exchange 2010 and Outlook Web App (OWA), which give teleworkers access to email, voice mail, instant messages, and SMS text messages from their Inbox using any of the major web browsers (Internet Explorer, Safari, Firefox, and Chrome).

Both of these solutions support the use of personal identity verification cards, if required.

SELECTING TELEWORK SERVICES AND APPLICATIONS

You might say the higher the risk profile, the fewer the services exposed for access. But that approach unnecessarily limits teleworker productivity. Risk profiles inform your decision-making process, but you can expect service delivery to evolve over time as your agency determines what works best.

By distilling your risk model to a discussion of endpoints and services irrespective of technology, you create a clear framework in which to refine necessary policies. Then you can ensure that the services and solutions you do provide are compliant. For example, take the relatively low risk case of a teleworker using a managed PC. You can require the use of a smart card to authenticate the user via SSL VPN and provide access through a portal, designing a solution that supports Homeland Security Presidential Directive 12 (HSPD-12) credentials, FIPS 201 specifications, and Office of Management and Budget (OMB) Memorandum 06-16 for safeguarding PII. You can add other technologies as needed to improve protection of information in transit and at rest.

When evaluating the services and applications to make available in telework scenarios, factor the following into your planning:

- **Mission impact.** How important is a particular service or application to your agency's mission? Weigh the business impact and consider COOP before limiting access to a service teleworkers could use.
- **Data classification.** Does a service or application use data that is classified, sensitive, sensitive but unclassified (SBU), or contains PII? Mission-critical applications, such as human resources systems and financial databases, may require special solutions for telework access.
- **Network bandwidth.** Is there adequate bandwidth to support extra teleworkers or computation-intensive applications? This includes your own network bandwidth in addition to the infrastructure from which teleworkers initiate access.

Data security from Microsoft

Microsoft provides many security-enhancing features in products you may already deploy. For example:

- Windows 7 BitLocker and BitLocker To Go are drive encryption technologies.
- Windows Vista BitLocker is the native encryption method for primary and secondary data.
- Encrypting File System (EFS) in Windows Vista and Windows XP SP3 prevents an intruder who gains unauthorized physical access to your encrypted files or folders from reading them.
- Rights Management Services in Windows Server 2008 and Windows Server 2003 work with RMS-enabled applications to help safeguard digital information from unauthorized use.
- Secure/Multipurpose Internet Mail Extensions (S/MIME) encryption in Exchange 2010 and Exchange Server 2007 helps protect the contents of email messages.

PERFORMING RISK ANALYSIS

Threat modeling is a key component of risk management. A model helps you to understand whether an endpoint or service is vulnerable and helps you to evaluate the types of attacks that could occur. You must determine the most appropriate method of risk assessment for your organization, along with a suitable threat taxonomy or categorization method.

To assess the risk of telework, you need a comprehensive view of systems, users, and transactions. Your threat model must assess whether:

- **Systems** have the properties of confidentiality, integrity, and availability. That is, data is available only to the people intended to access it; data and system resources are changed only in appropriate ways by appropriate people; and systems are ready when needed and perform acceptably.
- **Users** are authenticated and authorized correctly—their identity is established, and then they are explicitly allowed or denied access to resources.
- **Transactions** are non-repudiable, meaning that users can't perform an action and then later deny performing it.

STRIDE is an approach to threat categorization used in threat modeling that may help you assess the telework threat landscape and the risks to which your system will be exposed. It then provides a clear model for the discussion of enumerated threats and possible countermeasures or mitigations so you can weigh costs and risks in choosing your solutions.

To use the STRIDE approach, you break your system into relevant components—for example, telework endpoints, access points, and services. You can then analyze each component for vulnerability, breaking them into subsystems, if needed. In this way, you create a detailed map of the threat landscape so you can provide thoughtful and robust risk mitigation strategies.

STRIDE stands for security

A systematic approach to threat modeling, STRIDE was developed by Microsoft to categorize software threats. STRIDE stands for:

- ***S****poofing*, which means to illegally obtain access and use of another person's authentication information, such as a user name or password.
- ***T****ampering*, the deliberate destruction or manipulation of data.
- ***R****epudiation*, which is associated with users who deny performing an action.
- ***I****nformation disclosure*, or exposing information to users who should not have access to it.
- ***D****enial of service*, a malicious attack designed to prevent legitimate users from using a service or system.
- ***E****levation of privilege*, which opens the door to greater risk by granting unprivileged users privileged access to services or systems.

DEVELOPING A RISK MITIGATION STRATEGY

After conducting an appropriate risk assessment exercise, you should form a strategy for mitigating the risks associated with telework. STRIDE methodology may offer a framework for discussing a security strategy and can help you identify the applicable mitigations (shown in Table 4) to the threats revealed in the risk assessment process.

Microsoft and the threat landscape

The *Microsoft Security Intelligence Report (SIR)* provides an analysis of the constantly changing computer threat landscape based on the diverse and large-scale telemetry received by Microsoft from around the world . Download the full report at http://www.microsoft.com/sir.

Table 4. Identifying potential security responses for threats

Threat	Security property
Spoofing	**Authentication.** One solution is to use a gateway to authenticate users. For example, Forefront Unified Access Gateway offers help through the use of SSL.
Tampering	**Integrity.** Systems that support SSL provide mitigation for data tampering.
Repudiation	**Non-repudiation.** A system must be able to counter repudiation threats and include techniques, such as signing for a received parcel, so that the signed receipt can be used as evidence. Other solutions include enforcing the use of smart cards and email with S/MIME.
Information disclosure	**Confidentiality.** You need systems which ensure that information cannot be exposed to individuals who are not supposed to have access to it. One approach is to use a combination of SSL, smart card authentication to Active Directory, and Kerberos authorization services.
Denial of service	**Availability.** Server clustering is one solution.
Elevation of privilege	**Authorization.** You must deploy techniques that prevent an unprivileged user from contriving a way to be added to the administrators group. One solution is to combine smart card authentication to Active Directory with Kerberos authorization services and constrained delegation.

As a threat modeling example, suppose a teleworker sends data across the Internet through a gateway on the perimeter of your network. Three or four threat types in the STRIDE taxonomy can occur, as shown in Figure 1:

- The data flows may be tampered with (T).
- Systems may disclose information inappropriately (I).
- Denial of service attacks may render systems unavailable (D).
- Weak repudiation can threaten data stores (R).

With this understanding, you can choose the appropriate risk mitigations, such as detection and protection technologies, suited for your situation.

Benefits of threat modeling

- Threat modeling provides a repeatable process for finding and addressing threats to your services and systems accessed by teleworkers.
- It also gives you a head start on remediation planning.

Need help? Find resources for risk management on the Cybersecurity website.

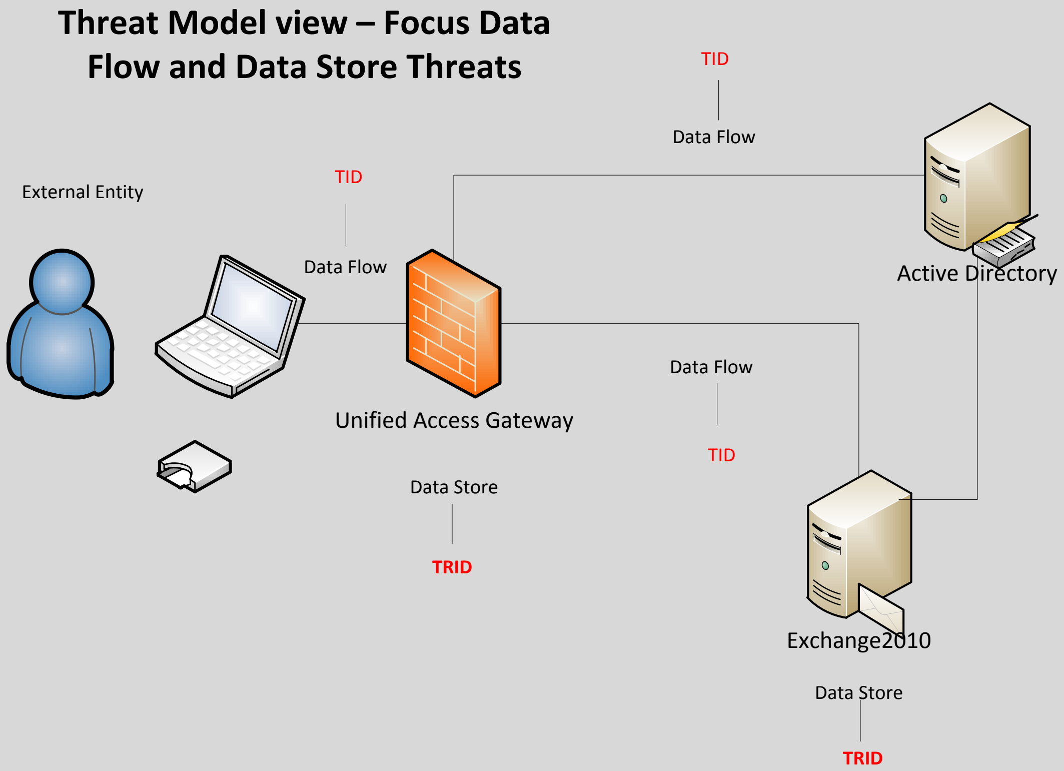


Figure 1. The STRIDE method helps you see where tampering (T), information disclosure (I), denial of service (D), and repudiation (R) may be problems during telework.

HOW MICROSOFT SUPPORTS TELEWORK

With careful planning, thorough checklists, and thoughtful guidelines, your IT staff can prepare for the risks associated with telework. Microsoft provides many technology solutions that both enable rich telework scenarios and help manage associated risks.

Microsoft approaches telework within the larger picture of cybersecurity for government. Telework represents a significant change in the way government does business, but it does not have to mean unnecessary risks. Your organization must adopt practices and tools that support a security life cycle of continuous monitoring and risk management.

We recognize that telework is an issue with technological and social implications, and we continue to work with industry and government partners to minimize the risks associated with new business requirements such as telework.

LEARN MORE

- For more information on the technologies and solutions discussed in this paper, please contact your Microsoft representative.
- To understand how Microsoft IT leverages these solutions to enable telework scenarios for our own employees, please see the TechNet IT Showcase website at: http://technet.microsoft.com/en-us/library/bb687780.aspx

Telework resources

Microsoft telework solutions allow you to change *where* you work without having to change *how* you work. Learn more: **http://www.microsoft.com/telework**

For more information

- **DirectAccess** is key to our remote access services for Microsoft IT users around the world. http://technet.microsoft.com/en-us/library/ee423652.aspx
- **Cybersecurity for Government** includes risk management strategies and advisory services. http://www.microsoft.com/govsecurity
- **Microsoft Security Response Center** offers security bulletins. http://www.microsoft.com/security/msrc
- **Microsoft TechNet Security TechCenter** provides how-to information about detecting, assessing, and removing threats. http://technet.microsoft.com/en-us/security/cc297183.aspx